

GeekBrains

Урок 5 Видео 2

Криптография

Подведение итогов

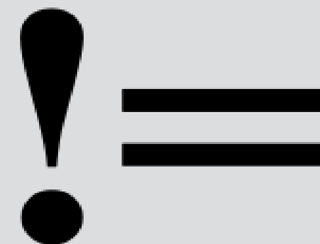
В этом видео

1. Обмен ключами шифрования
2. Потоковые шифры
3. Генераторы псевдослучайных последовательностей

GeekBrains

Проблему обмена симметричными ключами шифрования можно решить с помощью RSA





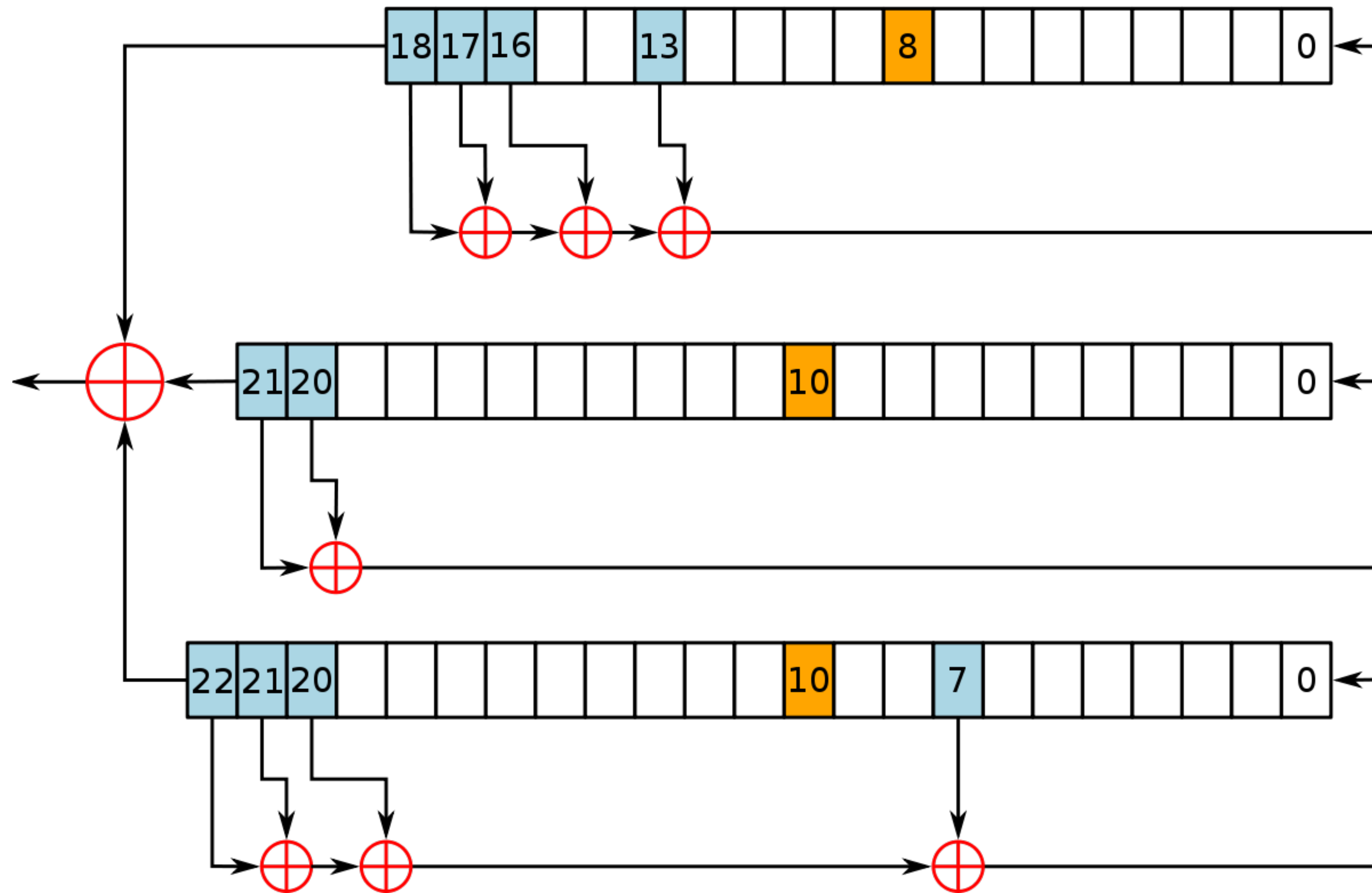


GeekBrains

Алгоритм Диффи-Хеллмана позволяет установить ключ шифрования при передаче данных по публичному каналу



Потоковые шифры



Разновидности потоковых шифров

С нелинейной комбинирующей функцией

С нелинейной фильтрующей функцией

Генераторы, основанные на управлении синхросигналом

Генераторы псевдослучайных последовательностей широко используются для создания ключей шифрования, nonce-ов, паролей и других секретов



Итоги

1. Don’t roll your own crypto
2. На практике научились эксплуатировать криптографические уязвимости
3. Научились пользоваться криптографическими библиотеками и инструментами
4. Знаете зачем нужны основные криптографические примитивы